UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X
UNITED STATES OF AMERICA,

Plaintiff,

-against-

MEMORANDUM AND ORDER
18 CR 457 (AMD) (CLP)

HUAWEI TECHNOLOGIES Co., Ltd., *et al.*,

Defendants.
----------X

POLLAK, United States Magistrate Judge:

Currently pending before this Court on referral from the District Judge are two letter motions[1] filed by the defendants Huawei Technologies Co., Ltd., Huawei Device Co., Ltd., Huawei Device USA, Inc., and Futurewei Technologies, Inc. (collectively, "defendants" or "Huawei"): 1) defendants' letter motion dated June 14, 2024, seeking certain relief relating to the Protective Order's treatment of SDM (the "SDM Motion") (ECF No. 432); and 2) defendants' June 14, 2024 letter motion seeking the Court's assistance in obtaining access to certain discovery restricted by the Bureau of Industry and Security ("BIS") of the U.S. Department of Commerce (the "BIS Motion") (ECF No. 433).

On September 10, 2024, this Court held oral argument on the motions. (See ECF No. 459). For the reasons set forth below, defendants' SDM Motion is granted in part and denied in part, and defendants' BIS Motion is denied.

BACKGROUND

Before addressing the two motions, the Court notes that a Protective Order relating to discovery was entered in this case on June 10, 2019, "after extended negotiations by the parties."

[1] A third letter motion was also filed on June 14, 2024, seeking to downgrade the government's February 7, 2022 disclosure letter from Attorneys' Eyes Only ("AEO") to Sensitive Discovery Material ("SDM") under the Protective Order (ECF No. 431). That motion was addressed in a separate order.

(ECF No. 442 at 2). The Protective Order provides for three levels of protection for discovery produced by the government: Discovery Material ("DM"), SDM, and AEO. (ECF No. 431 at 2 (citing P.O.[2] ¶¶ 1, 11, 16)). All discovery is designated DM, but if the government has a good-faith belief that greater restrictions are required, it may designate materials with an SDM designation, which is designed to protect highly sensitive information, including the identities of witnesses and victims, proprietary information of a victim financial institution, national security or law enforcement information, and information that could impede an ongoing law enforcement operation or implicate the safety of others. (ECF No. 442 at 2-3 (citing P.O. ¶ 19)). There are certain restrictions placed on defendants' review of SDM, including the ability to review it and discuss it only in the presence of counsel, and restrictions on possession of such information, including a prohibition from taking it outside the United States. (ECF No. 432 at 2 (citing P.O. ¶¶ 11-15)).

The Protective Order requires the government to establish good cause if a designation is challenged. (Id.)

DISCUSSION

I. Defendants' Motion For Relief Regarding the Treatment of SDM

Defendants' first motion, filed on June 14, 2024, seeks relief from the Court from certain restrictions in the Protective Order relating to SDM. (ECF No. 432 at 1). According to defendants, the parties have agreed to modify the Protective Order to allow the following: 1) defense counsel may share attorney work product and related emails describing SDM with Huawei in Mainland China, so long as the materials redact any verbatim quotes from the SDM and any Personally Identifiable Information ("PII"); 2) Huawei employees in China may discuss

[2] Citations to "P.O." refer to the parties' Protective Order filed on June 10, 2019 (ECF No. 57), and So Ordered by the Court on June 11, 2019.

SDM in the physical or remote presence of defense counsel, with the same proviso as above; 3) Huawei and potential witnesses may access SDM from defense counsel's Hong Kong offices through a technical solution which retains all SDM and related work product in the United States. (Id.) Despite these agreed-upon modifications to the Protective Order, defendants raise additional concerns that they have not been able to resolve in their discussions with the government. (Id.)

A. Remote Access in China

1. The Parties' Submissions

Defendants first complain that the Protective Order does not allow Huawei to show or discuss SDM with any potential witness in China. (Id. at 1-2). Since many of the witnesses are retired or no longer with Huawei and are unable or unwilling to travel to Hong Kong, defendants request that the Protective Order be modified to allow for a limited remote-review protocol in Mainland China similar to the protocol agreed to with respect to remote review in Hong Kong. (Id. at 2). Defendants contend that it will be important to review the SDM with the witnesses in order to ask them about the contents of certain documents or refresh their recollection of events that occurred many years earlier. (Id.) Defendants ask the Court to modify paragraph 12 of the Protective Order to provide:

> Notwithstanding any other provision of this Protective Order, Sensitive Discovery Material may be reviewed by a witness (including a potential witness) and/or a witness's counsel in any location in the presence of Defense Counsel or Defense Staff on a dedicated laptop or tablet configured to access a remote desktop operating in the United States over an end-to-end encrypted connection. Such laptop or tablet shall remain at all times in the custody of Defense Counsel or Defense Staff, and shall remain when not in use within the office of Defense Counsel.

(Id. at 7).

In response, the government submitted a letter dated July 15, 2024, indicating that since the entry of the Protective Order in 2019, the government has already agreed to significant modifications in order to accommodate the concerns raised by defendants. (ECF No. 442 at 2).

Under the Protective Order, SDM and work product derived from SDM was originally to be reviewed in the United States only, and Huawei employees were authorized to seek safe passage to review these items in the United States. (Id.) According to the government, safe passage to the United States has been freely granted to employees and to Huawei in-house counsel. (Id.)

However, in July 2023, in an effort to address defendants' concerns regarding the burden of requiring Huawei personnel and witnesses to travel to the United States to review SDM with counsel, the government agreed to modify the Protective Order to allow SDM to be accessed from and discussed in Japan, South Korea, the European Union, the United Kingdom, Canada, Mexico, and Switzerland. (Id. at 3). The government also agreed to allow defense counsel to share work product describing SDM with client personnel regardless of the client's location. (Id.) In May 2024, the government agreed that defendants' personnel could have face-to-face conversations in China about work product derived from SDM, in the presence of defense counsel, with the exception of PII. (Id.) Most recently, in June 2024, the government agreed to allow remote access to SDM materials from the Hong Kong office of defendants' counsel, Sidley Austin LLP. (Id.)

The Protective Order also contains a provision that if an individual permitted to review SDM is not able to travel to the United States or any of the other agreed-upon locations, the parties are to "confer to devise a means for the [individual] to review [SDM]" outside these various locations. (Id.) The government represents that defendants have not identified any

specific individual who is unable to travel to any of the locations, just that it may be burdensome for them to do so. (Id.) Moreover, pursuant to the Protective Order, the parties agree to a process whereby if defendants request that a document designated as SDM be de-designated, the government is to seek judicial intervention if the parties cannot agree. (Id.) According to the government, it has not filed any such motions because discussions with defendants' counsel were ongoing and defendants indicated they would be filing the instant motion. (Id. at 3 n.2).

The government contends that the restriction limiting access of SDM in Mainland China is designed to protect important government interests, and the government reiterates its concerns that the PRC government "seems willing to take actions that appear designed to impede this prosecution." (Id. at 5). The government is concerned that surveillance in the PRC will lead to disclosure of the SDM materials, including disclosure of materials that could jeopardize the safety of witnesses and sources, particularly those in or with family in the PRC. (Id.) Moreover, under PRC law, the Chinese government could compel individuals in the PRC to disclose those SDM materials, resulting in efforts to tamper with witnesses. (Id.) Under the PRC's National Intelligence Law, a PRC intelligence agency may compel PRC entities to secretly share access to the data of a U.S. business or entity and to create backdoors into equipment and software sold abroad; indeed, new PRC laws prohibit foreign companies operating in China from using encryption software and require these entities to store data in China. (Id. at 7 (quoting U.S. Dep't of Homeland Security, Office of Strategy, Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment From Firms Linked to the People's Republic of China at 6-7 (Dec. 22, 2020))).[3] With respect to Huawei specifically, the government asserts that Huawei is mandated by legislation and political reality to comply with

[3]See https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

an order from the PRC government or the communist party to do its bidding in any context. (Id. (citing various experts)).

The government notes that its concerns are consistent with not only threat assessments of the U.S. intelligence community, but with businesses and universities, which see the PRC as "an information-security threat." (Id. at 6); see Annual Threat Assessment of the U.S. Intelligence Community at 11 (Feb. 5, 2024) (stating that "China remains the most active and persistent cyber threat to U.S. Government, private-sector, and critical infrastructure networks").[4] The Office of the Director of National Intelligence has warned that PRC laws since 2015 have "'provide[d] the PRC government with expanded legal grounds for accessing and controlling data held by U.S. Firms in China,'" (id. at 7 (quoting ODNI, Nat'l Counterintelligence & Security Center, Safeguarding Our Future; U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies at 1 (June 20, 2023))),[5] and the U.S. Department of Commerce's International Trade Administration has issued a cautionary warning to individuals traveling to the PRC that they have "'no expectation of privacy in public or private locations.'" (Id. at 6 (quoting U.S. Dep't of Commerce, Int'l Trade Admin., China – Country Commercial Guide: Business Travel (Apr. 7, 2023))).[6] Their advice to travelers is to bring only the minimum of electronic equipment, explaining that "'[a]ll hotel rooms and offices are subject to on-site or remote technical monitoring at all times.'" (Id.)

Finally, according to the government, disclosure of SDM material containing intellectual property would further victimize the companies whose intellectual property is already at issue in

[4] See https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf.

[5] See https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.

[6] See https://www.trade.gov/country-commercial-guides/china-business-travel.

this case. (Id. at 5). Thus, the restrictions on disclosure of such materials in Mainland China are designed to mitigate these risks, and defendants have not argued otherwise. (Id.)

As a result of the significant risk that the PRC government would be able to obtain SDM and use it in the various ways of concern identified by the government, the government opposes the defendants' request to allow remote access in Mainland China to SDM stored in the United States, even under the proposed protocol of a laptop with an encrypted application similar to the one agreed to for remote access in Hong Kong. (Id. at 8). The government contends that it has shown good cause for resisting this proposal, particularly in light of the fact that the PRC government could compel defendants and defense counsel to provide the PRC government with the laptop, regardless of the Protective Order, and that there is a substantial risk that the PRC government could hack the computer to obtain SDM material, despite the technical protections envisioned. (Id.)

In reply, defendants argue that the government's proffered security concerns are not actually implicated by defendants' proposal. (ECF No. 450 at 1). Defendants insist that under their proposal, no SDM would enter Mainland China. Similar to the protocol in Hong Kong, defendants explain that SDM would "remain at all times on a secure server in Oak Brook, Illinois," and the material would only be viewable in Mainland China over an "encrypted, dedicated connection streaming still images of a remote desktop at a rate of 30 frames per second." (Id. at 3 (citing Tyrrell Decl.[7] ¶¶ 10-11)). Thus, if the Chinese government were to force Huawei or its counsel to turn over the laptop or related material, the laptop would no longer

[7] Citations to "Tyrrell Decl." refer to the Declaration of Jason Tyrrell, Director of Litigation and Practice Support Services at Sidley Austin LLP, executed on June 13, 2024, which details the defendants' proposed security protocol and is attached to defendants' SDM Motion as Exhibit A (ECF No. 432-1). According to the Declaration, Mr. Tyrrell has been at the firm since 2005, and is responsible for the firm's e-discovery technology operations and has managed thousands of project-specific technology protocols to enable remote secure document review. (Tyrrell Decl. ¶ 1).

contain the SDM. (Id.) In addition, even if the PRC were to hack into the encrypted stream, they would only be able to view one single image of the material reflected on the desktop in that moment; moreover, defendants argue that the protocol they propose is virtually impossible to hack, likening it to putting a human on Mars. (Id. at 3-4). This protocol would be "technically the same" as the one already implemented in defense counsel's Hong Kong offices. (Id. at 4).

Given that the government's security concerns are, in defendants' view, largely speculative, defendants argue that these concerns do not outweigh the likelihood of the prejudice to Huawei as a result of the restriction, and the government has therefore failed to establish good cause. (Id. at 4-5). Defendants reiterate that "[e]xperience already confirms" that they will be unable to interview potential witnesses located in Mainland China who either refuse to travel or cannot because of impediments such as health, age, or familial obligation. (Id. at 5). In addition, defendants take issue with the government's assertion that the restriction is necessary given Huawei's history of obstruction in the instant case, when this obstruction is nothing more than "vague *allegations* in the S3 Indictment" that have not yet been proven. (Id.) (emphasis in original).

At oral argument, the government challenged defendants' characterization of the security protocol in their reply, saying that the suggestion that SDM will never enter Mainland China is mere "semantics." (Tr.[8] at 19:8). Even with the information displayed as encrypted images on a computer screen, the information still is viewable in Mainland China; indeed, that is "the whole point of the protocol." (Id. at 19:9-14). The government emphasized that, at the time of these witness interviews, with witnesses viewing the screen, the PRC could monitor the laptop and access the SDM displayed thereon. (Id. at 20:14-24). The government noted that the U.S.

[8] Citations to "Tr." refer to the transcript of the oral argument held on the SDM Motion and BIS Motion on September 10, 2024 (ECF No. 463).

Department of Commerce's international trade administration in 2023 found that hotel rooms and offices in Mainland China specifically are subject to remote monitoring at all times, and the U.S. Embassy in China receives regular reports of Mainland China's monitoring of U.S. citizens. (Tr. at 20:25-21:8). Thus, because of the particular concern with the monitoring in Mainland China, even stationing the computer in an office in Mainland China and having witnesses travel there constitutes a larger security risk than utilizing the protocol in Hong Kong. (Id. at 21:14-25). In addition, the government emphasized that the Hong Kong protocol was, in its view, a "very significant compromise," and it is not inclined to extend such compromise even further, to what it describes as an "unacceptable risk." (Id. at 23:4-11).

Further, the government reiterated that defendants should first utilize the procedure outlined in the Protective Order, which provides that when defendants identify a particular individual who is unable to travel to any of the designated locations for an interview to review the SDM, the parties are to confer to devise a plan for that individual to review the SDM another way. (Id. at 24:1-25). Thus, defendants' instant request is premature, given that they have not identified with any particularity an individual who cannot view the SDM under the current restrictions. (Id. at 23:18-22).

During oral argument, defendants raised a concern that if they were required to confer with the government regarding particular witnesses to be interviewed, that would reveal defendants' protected work product. (Id. at 25:3-10). Additionally, defendants note that they filed this motion as a way to expedite the process for interviewing potential witnesses, concerned that as trial draws nearer, they will not have the time to follow the procedure contemplated in the Protective Order. (Id. at 27:24-28:2). The government responded that it has a filter team in place to facilitate conferences with defendants to protect work product, and confirmed that the

filter team can be ready "at a moment's notice" to address defendants' timing concerns. (Id. at 28:6-10).

2. Analysis

Under Rule 16 of the Federal Rules of Criminal Procedure, a court may, "for good cause, deny, restrict, or defer discovery or inspection[,]" particularly considering "the safety of witnesses and others, a particular danger of perjury or witness intimidation, the protection of information vital to the national security, and the protection of business enterprises from economic reprisals." Fed. R. Crim. P. 16(d)(1) and Fed. R. Crim. P. 16 advisory committee's note to 1966 amendment; see also United States v. Smith, 985 F. Supp. 2d 506, 522 (S.D.N.Y. 2013) (applying Rule 16(d) to a request for a protective order and collecting cases saying the same). While the defendant has a Sixth Amendment right to consult with counsel in the preparation of his defense, under certain circumstances, the court may impose restrictions on the defendant's access. See United States v. Guzman Loera, 24 F.4th 144, 154-55 (2d Cir. 2022) (approving protective order that prohibited discovery from being removed from the United States when it included witness statements, witness identifying information, and information related to ongoing investigations and law enforcement techniques); In re Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 122 (2d Cir. 2008) (noting that Rule 16(d) "leaves the precise conditions under which the defense may obtain access to discoverable information to the informed discretion of the district court").

The "good cause" standard set out in Rule 16(d) requires the party seeking a protective order to demonstrate that "disclosure will result in a clearly defined, specific and serious injury." In re Terrorist Attacks on September 11, 2001, 454 F. Supp. 2d 220, 222 (S.D.N.Y. 2006) (quoting Shingara v. Skiles, 420 F.3d 301, 306 (3d Cir. 2005)); United States v. Smith, 985 F. Supp. at 522-23 (collecting cases, noting that the burden rests on the party seeking the proposed

restrictions to demonstrate good cause, and the Court should consider whether the dissemination of the materials at issue would "inflict[] 'hazard to others,' and whether the 'imposition of the protective order would prejudice the defendant'") (quoting United States v. Carriles, 654 F. Supp. 2d 557, 566 (W.D. Tex. 2009) (further citations omitted))).

The good cause standard applies even when the parties previously stipulated to a protective order. United States v. Smith, 985 F. Supp. 2d at 523 (quoting United States v. Luchko, No. 06 CR 319, 2006 WL 3060985, at *3 (E.D. Pa. Oct. 27, 2006)). Indeed, under the terms of the instant Protective Order, upon a party's challenge to a protective designation, the party seeking protection must establish good cause. (P.O. ¶ 19). As noted, factors a court may consider in allowing a restriction of discovery material include witness safety, concerns of possible witness intimidation, and national security concerns. Fed. R. Crim. P. 16 advisory committee's note to 1966 amendment; see also United States v. Aref, 533 F.3d 72, 78 (2d Cir. 2008) (holding that Rule 16 "authorizes district courts to restrict discovery of evidence in the interest of national security"). In cases involving the theft of trade secrets, the Third Circuit has noted that 18 U.S.C. § 1835(a) "'represent[s] a clear indication from Congress that trade secrets are to be protected to the fullest extent.'" (ECF No. 442 at 5 (quoting United States v. Hsu, 155 F.3d 189, 197 (3rd Cir. 1998))).

Information in this case is designated SDM when it implicates, for example, the identities of witnesses and victims, national security information, or information that threatens an ongoing investigation or the safety of others. (ECF No. 442 at 2-3; P.O. ¶ 19). The government has detailed concrete and serious security threats surrounding the viewing of SDM in Mainland China, particularly given the PRC government's surveillance of hotel rooms and offices and monitoring of U.S. citizens in the area. At oral argument, the government outlined a scenario in

which a member of the PRC, or even an interviewee themselves, could, through hidden video cameras or similar surveillance technology, monitor the laptop screen displaying SDM and provide it to the PRC, even with the vast protections afforded by the defendants' proposed protocol. (Tr. at 20:14-21:8). Given the risks of interception of this sensitive material, not only to witnesses but to the trade secrets of financial institutions and victims and to national security concerns, if it were to be displayed in Mainland China, the Court finds that the government has established good cause for the current prohibition on SDM materials traveling to or being viewed in Mainland China. See United States v. Aref, 533 F.3d at 78 (holding that protecting information "'vital to the national security'" meets Rule 16's "good cause" standard (quoting Fed. R. Crim. P. 16 advisory committee's note to 1966 amendment)).

Further, when balanced against the government's interest in minimizing the potential security threat, the risk of prejudice to defendants appears relatively low. The government has made several concessions to allow for defendants' interviews with potential witnesses, allowing Huawei personnel free passage to the United States to view SDM, as well as allowing SDM to be reviewed in over six foreign countries. (ECF No. 432 at 4, 4 n.2). In addition, defendants have not shown that they have actually been hampered by this restriction, as they do not identify any particular instance where an individual they wished to interview could not or would not travel from Mainland China, simply stating generally that "[e]xperience already confirms . . . that many of these individuals will not voluntarily travel . . ." (ECF No. 450 at 5). Thus, defendants' request is premature, especially considering that the Protective Order provides a means by which defendants can confer with the government to devise a plan to interview these individuals when necessary. Given the government's assertion that their filter team will be promptly available should defendants wish to utilize the procedure agreed to in the Protective Order, it appears that

defendants' key concerns, regarding work product, timing, and the overall opportunity and feasibility of interviewing potential witnesses in Mainland China, are all adequately addressed by the Protective Order's current procedures. Defendants' request to amend the Protective Order to allow SDM access in Mainland China is therefore denied, without prejudice to renew at such time when specific issues arise that cannot be resolved under the procedures provided in the Protective Order.

B. Defendants' Request For a De-Designation Period

Defendants also seek to modify the Protective Order to establish a process for resolving disputes over whether SDM has been properly designated. (ECF No. 432 at 7-8). Defendants specifically seek to modify the Protective Order to (1) set a fixed period of time in which the government, upon receipt of a de-designation request, is required to either de-designate or demonstrate the propriety of the designation to the Court, and (2) clarify that the government must "have a specific and articulable basis to believe that the DM restrictions alone are insufficient to address any legitimate governmental interest." (Id.) Defendants propose to insert certain text, in the following provision:

> Any documents, material, or information may be designated [SDM] only upon a good-faith belief by the government that *(1)* such materials contain identifying information for any potential witness, victim or individual not a party to this litigation; proprietary or sensitive information of a victim financial institution or of a witness; national security or law enforcement sensitive information; information that could implicate the safety of others; information that could impede an ongoing law enforcement investigation; and/or any other information that the government deems in need of heightened protection under this Protective Order; *and (2) that less restrictive means would not be sufficient to protect a legitimate public interest in confidentiality*. If the government and Defense Counsel do not agree that certain material should be designated as [SDM], the defendants may provide notice to the government and a reasoned explanation regarding why the defendants do not believe the material require treatment as [SDM]. To the extent that the parties do not agree, the government *must*

> make an application to the Court *within 21 days of being so notified by the defendants* and seek to establish good cause regarding why the material should be treated as [SDM]. *If the government timely files a motion to confirm its designation of the material,* the defendants shall treat the material as [SDM] pending any determination by the Court.[9]

(Id. at 8).

1. Set Period For De-Designation Determinations

a) The Parties' Arguments

According to defendants, over 36% of the discovery, or over 1.5 million documents, provided by the government have been designated as SDM. (Id. at 2). Although defendants have identified numerous documents that have been over-designated, they contend that they have had difficulty getting the government to de-designate them. (Id. at 3, 8). Defendants note that the SDM restrictions have proven to be more burdensome that originally thought, and although the Protective Order contemplates the government having the burden to verify the propriety of the SDM designation, the government has never applied to the Court when faced with a challenge, having the practical effect of "shift[ing] the burden to the defense to prove the impropriety of each SDM designation." (Id. at 3). Huawei claims to have attempted to mitigate the problem by specifically identifying documents for de-designation; this has resulted in the de-designation of 27,302 documents out of the 28,678 requested by defendants. (Id.) Defendants contend that having to identify those SDM documents that defendants feel are most important reveals defense strategy. (Id.) While defendants acknowledge the government's legitimate interest in confidentiality, defendants contend that the government has not demonstrated that the burdens faced by defendants in reviewing this SDM material are consistent with Rule 16, and that the restrictions have not been "tailored to mitigate the risk of 'a clearly defined, specific and

[9] Defendants' proposed amendments to the Protective Order language are italicized.

serious injury.'" (Id. at 7 (quoting United States v. Castricone, No. 20 CR 133, 2021 WL 841405, at *1 (W.D.N.Y. Mar. 5, 2021) (further citations omitted))). In addition, defendants note that the government often takes several months to review these de-designation requests, and in one instance, took almost a year. (Id. at 3 n.1).

In responding to the defendants' request to modify the Protective Order to establish a set period of 21 days in which the government must respond to a defense request to de-designate SDM or move the Court for relief, the government contends that in each instance where the defendants request de-designation, the government not only reviews the documents but solicits the input of others, such as victims or witnesses, whose interests may be implicated, and proposes compromises to enable information sharing with the defendants. (ECF No. 442 at 10). The government asserts that the length of time required to conduct this analysis varies dependent on the number of documents involved, the number of interested parties, and the response time of those interested parties to the government's inquiries. (Id.) Requiring the government to respond in 21 days will impair the government's ability to consult with victims and witnesses and to negotiate solutions to any issues. (Id. at 11). Thus, the government contends that it has established good cause for not modifying the Protective Order to require responses in 21 days – "or, indeed, any specific period." (Id.) At oral argument, the government emphasized that setting any specific time period within which the government must respond or seek an extension from the Court would be "overly burdensome" given the variability of the government's ability to investigate these requests. (Tr. at 32:9-16).

The government further argues that defendants have not shown any actual prejudice, nor have they demonstrated that any such prejudice outweighs the government's concerns. (ECF No. 442 at 11). Notably, defendants can review and use SDM discovery while the government is

reviewing the request to de-designate and, in light of the modifications to the Protective Order, review of such discovery is now possible outside the United States in the various countries identified above. (Id.) To the extent that defendants have cited cases in support of their motion, the government distinguishes those cases by noting that in none of them was the government required to respond to de-designation within a specific time period. (Id. at 12 (citing United States v. Ramirez, No. 21 CR 41, 2021 WL 914457, at *2 (S.D.N.Y. Mar. 10, 2021); United States v. Jackson, No. 21 CR 537, 2022 WL 582700, at *1-2 (S.D.N.Y. Feb. 25, 2022); United States v. Castricone, 2021 WL 841405, at *2)).

In reply to this point, defendants contend that the government's incomplete explanations for its delay in responding to de-designation requests "only underscore the need for clear guidelines," and emphasize that even narrow de-designation requests have taken months to resolve with little explanation. (ECF No. 450 at 8). Defendants concede they would be amenable to a time period of longer than 21 days (id.), but, at oral argument, emphasized that they believe it would "operate more efficiently for all concerned" if there were a set deadline that could be extended on request, rather than the open-ended procedure currently in place. (Tr. at 34:14-17).

b) Analysis

With respect to defendants' request to set a deadline for the government to respond to de-designation requests, the Court notes that a trial date has been set for January 2026 (Tr. at 9:17-18), and the defendants are entitled to know when to expect the government's decision on these requests for de-designation so they may prepare for trial accordingly. Such notice is necessary for defendants to adequately prepare investigations and arrange interviews with full knowledge of how they may use certain related discovery materials. The government's varied and lengthy response times underscore the need for a set deadline to keep defendants informed on the

process. At the same time, the Court is sensitive to the government's explanation that investigating de-designation requests takes substantial time and resources, given the government often must confer with multiple third parties about sensitive issues. Therefore, the Court denies the defendants' request to impose a 21-day deadline but, instead, Orders the government to respond to a de-designation request within 60 days of receipt of the request or, if the government cannot meet the 60-day deadline, the government must confer with defendants and come to an agreement on an appropriate extension of time. In the event the parties fail to agree, the government may file a request for an extension of time with the Court.

2. Proposed Modification to the Definition of SDM

a) The Parties' Arguments

Defendants' second request involves a proposed modification to the definition of SDM that would require the government to determine that "less restrictive means [than the SDM designation] would not be sufficient to protect a legitimate public interest in confidentiality." (ECF No 432 at 8). The government argues that the current definition, which requires a good-faith belief that the discovery includes certain sensitive information, does not impose an undue burden on defendants, whereas the proposed "least restrictive" designation would require the government to work with victims and third parties in a way that would not only be unduly burdensome, but also likely to chill future cooperation in this and other cases. (ECF No. 442 at 13). Although there has been a large volume of material designated as SDM, the government argues that this is to be expected given the nature of the charges involving fraud on various financial institutions, and the theft of intellectual property from numerous businesses. (Id.) Moreover, defendants' counsel have already extensively negotiated the provisions of the Protective Order to include the designation of SDM, and the government has shown a willingness to modify the terms where feasible. (Id.) Thus, in the absence of a showing of

actual harm based on the current provision for designating SDM, the government argues that imposing this new burden is unwarranted. (Id.)

In reply, defendants argue that the government has been overbroad in its designation of SDM, designating as such "documents that were publicly available, Huawei's own documents, and other materials," including some that were created or existed in Mainland China.[10] (ECF No. 450 at 6, n.4). Defendants contend that the government is inappropriately holding this non-SDM under excessive restrictions for long periods of time and therefore is not following the Protective Order's procedure for designating heightened confidentiality restrictions. (Id. at 6 (citing P.O. ¶ 19)). Defendants complain that the Protective Order's categories for SDM are so broad that they could be stretched to "absurd conclusions," and although the government has never gone to such extremes in practice, defendants are concerned by the government's sweeping treatment of SDM designations nonetheless. (Id. at 7). Defendants therefore suggest that their request is necessary, and ask for the Court to clarify that the government's burden to establish "good cause" includes the showing that, for SDM designation, the material is not sufficiently protected as DM. (Id.)

b) Analysis

As to defendants' request for clarification of the standard required for the government to show "good cause" for SDM when challenged under the Protective Order, the Court notes that, as expressed at oral argument, the SDM designation is to be used only when the DM designation is insufficient to protect the interests implicated by the discovery material. (Tr. at 35:14-16). This seems clear under the Protective Order's language that the government must have a "good-faith belief" that the material fits within the SDM categories, and ultimately that the government

[10] See n.11, *infra.*

must show "good cause" for the heightened restriction if challenged. (See ECF No. 450 at 7 (citing P.O. ¶ 19)). In light of this, along with defendants' concession that the government has not abused the Protective Order's broad designation language (id.), the Court declines to order the defendants' requested amendment to the Protective Order, but notes that, under the existing language of the Protective Order, the government must establish good cause for a challenged SDM designation, and, by necessity, must show that the DM designation is insufficient to provide protection for the interests implicated by the material.[11]

II. Defendants' Request For Relief Related to BIS Licensing Restrictions

Defendants' second letter motion, dated June 14, 2024 (ECF No. 433), relates to the inclusion of Huawei and certain non-U.S. affiliates on the "Entity List" maintained by the U.S. Department of Commerce, which prohibits the export to Huawei of any technology, including technology contained in the government's discovery materials, in the absence of a license issued by the Bureau of Industry and Security ("BIS"). (ECF No. 433 at 1). Specifically, defendants argue that BIS imposed an "unwarranted" restriction on approximately 536,000 discovery documents in this case, and they request the Court's assistance in obtaining access to these documents consistent with the Protective Order. (Id.)

A. Commerce Department Export Controls

Under the Export Control Reform Act of 2018 ("ECRA"), the Secretary of Commerce is given the authority to promulgate regulations to control the export, re-export, and in-country transfers by U.S. or foreign persons of specific categories of items and information, including commodities, software, and technologies from the United States to foreign countries. 50 U.S.C.

[11] To the extent that the defendants have specific examples of publicly filed documents or Huawei's own documents that are marked SDM, defendants should raise the issue with the government in accordance with the terms of the Protective Order. The government should then either de-designate these documents or respond by demonstrating to the Court why they deserve SDM treatment, as it is presently unclear why such documents would require designation as SDM. (See ECF No. 450 at 6).

§§ 4801-4852. (See Borman Decl.[12] ¶¶ 10, 11, 12). ECRA provides that export controls are to be used "only to the extent necessary to restrict the export of items that would make a 'significant contribution to the military potential of any other country. . . which would prove detrimental to the national security of the United States' or 'further significantly the foreign policy of the United States or [its ability] to fulfill its declared international obligations.'" (Borman Decl. ¶ 11 (quoting 50 U.S.C. §§ 4811(1)(A)-(B))). The Export Administration Regulations ("EAR"), 15 C.F.R. §§ 730-774, restrict the export of certain technologies that could be detrimental to the national security or foreign policy of the United States, and impose licensing restrictions for the lawful export or re-export of certain technologies depending on the nature of the technology or item, the country of destination, and the end use of the item. (Id. ¶¶ 5, 6, 16, 17, 19). The EAR includes a specific list of controlled items for which a license may be required to export the item from the United States. (Id. ¶¶ 19, 22, 23). For violations of the regulations, ECRA and the EAR provide for criminal and civil penalties, including monetary penalties and denial of export privileges. (Id. ¶ 25).

BIS is an agency within the Department of Commerce ("Commerce") that is responsible for controlling the export, re-export, and in-country transfer of items subject to the EAR. (Id. ¶ 5). As part of BIS's responsibilities, it licenses the export, re-export, and in-country transfer of items subject to the EAR and it maintains the Commerce Control List ("CCL") to "ensure the appropriate administration of export controls." (Id. ¶ 7).

[12] In opposition to the defendants' motion, the government has submitted the Declaration of Matthew S. Borman, Principal Deputy Assistant Secretary for Strategic Trade and Technology Security, United States Department of Commerce, dated July 15, 2024 ("Borman Decl.") (ECF No. 443-1). According to Mr. Borman, his duties include implementing BIS's controls on "the export of dual-use and military items for national security and foreign policy reasons," as well as overseeing BIS's programs "to ensure that industrial resources are available to meet national and economic security requirements." (Borman Decl. ¶ 1). Mr. Borman also oversees BIS's implementation of the Chemical Weapons Convention and Additional Protocol to the US-International Atomic Energy Agency Agreement. (Id.)

When a license is required from Commerce, the "applicant" for the license must be the U.S. principal party seeking to export the item, and "principal party" is defined as "'[t]hose persons in a transaction that receive the primary benefit, monetary or otherwise, of the transaction. Generally, the principals . . . are the seller and the buyer.'" (Id. ¶ 23 (quoting 15 C.F.R. § 772.1)). According to Principal Deputy Assistant Secretary Borman, a license application is "subject to a thorough interagency review process" which authorizes the Departments of State, Defense, and Energy to review license applications submitted to Commerce and allows the expertise of these other agencies to be included in the review process "to ensure only those exports that are consistent with U.S. national security and foreign policy interests will be approved." (Id. ¶ 24). License applications must identify the technology or software being exported, provide the ECCN from the CCL, identify the end-user, the end use, and the purpose for export, and provide supporting documentation. (ECF No. 443 at 3).

Pursuant to the EAR, an "Entity List" has been created which imposes licensing requirements on listed entities beyond those found in the Regulations, including limitations on the use of license exceptions. (Borman Decl. ¶¶ 26, 28). In order to export any technology to a listed entity, the exporter must obtain a license from BIS to do so. (ECF No. 443 at 3). For example, even if no license is required to export an item to China, a license may be required if the item is destined for an entity on the Entity List. (Borman Decl. ¶ 28). According to Mr. Borman, Huawei Technologies and certain non-U.S. affiliates were added to the Entity List on May 16, 2019. (Id. ¶ 29). As a result, there are now additional licensing requirements imposed on exports, re-exports, and transfers of items subject to the EAR that are destined to or involving Huawei entities. (Id.) The addition of Huawei to the Entity List was based on "'reasonable cause to believe that Huawei has been involved in activities contrary to the national security or

foreign policy interests of the United States.'" (Id. ¶ 30 (citing 84 Fed. Reg. 22961)). In rules promulgated by BIS in 2020, additional restrictions were placed on foreign produced products if destined to a listed Huawei entity or where Huawei was involved in the transaction. (Id. ¶ 31).

B. The Parties' Submissions

1. Defendants' Request for Assistance

According to defendants, the addition of Huawei and various related entities to the EAR Entity List occurred in May 2019, shortly before the finalization of the Protective Order. (ECF No. 433 at 1). Since software and "technology," which is broadly defined to include "'[i]nformation necessary for the 'development,' 'production,' 'use,' operation, installation, maintenance, repair, overhaul, or refurbishing . . . of an item,'" are subject to EAR controls, any type of technical information contained in any document cannot be provided to Huawei without authorization from BIS. (Id. at 3 (citing 15 C.F.R. § 774, supp. 1, cat. 3; 15 C.F.R. § 772.1)). Defendants contend that by law, the Department of Justice ("DOJ") is prohibited from providing any discovery that contains technology subject to EAR. (Id. at 2).

Defendants contend that although under the Federal Regulations, DOJ is the "principal party in interest" because it is required to satisfy its discovery obligations to Huawei in this prosecution, and therefore is the appropriate party to obtain the BIS license, the government has not made an application, asserting instead that it is defendants' responsibility to obtain the necessary license. (Id. at 3-4). See 15 C.F.R. § 758.3(a); see also 15 C.F.R. § 740.11(b). Defendants represent that although they have been granted certain limited authorizations[13] to

[13] These authorizations are distinct from BIS licenses. As detailed in the Borman Declaration, BIS, in response to defendants' requests for "expedited treatment in light of near-term litigation deadlines," issued to defendants letters of authorizations permitting export of certain discovery in the litigation "without requesting that Huawei's counsel formally apply for a license." (Borman Decl. ¶ 37). Subsequent references to "authorizations" in this Order refer to these expedited authorizations granted by BIS to defendants, rather than the licenses that BIS grants after its thorough review process.

share specific discovery with Huawei, for over two years they have tried to obtain a broader BIS license without success, thus limiting their ability to share the government's discovery with Huawei, despite the Protective Order. (Id. at 1).

Specifically, defendants represent that on July 8, 2022, they submitted a request to BIS seeking authorization to release all of the documents produced by DOJ to Huawei for purposes of the defense in this case, subject to the Protective Order provisions. (Id. at 4). Defendants explain that although they have received limited authorizations to share some materials containing EAR-controlled technology, there are over 2 million documents[14] that have been withheld from Huawei personnel involved in the case because the documents may contain EAR technology that may not be covered by those limited authorizations. (Id.) This has placed a burden on defendants' counsel to review each document to determine if a license is needed before they can share the document with their client. (Id.) After extensive negotiations, BIS issued an Interim Authorization in October 2023, granting permission to share certain discovery with Huawei but only under the SDM conditions. (Id. at 4-5). Defendants contend that this subjects the 536,000 documents already determined by DOJ to warrant the lower DM designation to the much more onerous restrictions imposed on SDM. (Id. at 5). When defendants continued to press for additional authorization, BIS, on January 19, 2024, requested that Huawei resubmit its July 8, 2022 authorization request, which it did, only to have it returned on March 29, 2024 without action, effectively denying it. (Id.)

BIS indicated that for Huawei to obtain permission to gain full access to the discovery documents, defense counsel would need to identify potential "technology," determine if it contained "development," "use" or "production" technology, classify the technology in

[14] Defendants claim that of these 2 million documents, 536,000 of them have been designated by the prosecution as DM, with the remaining 1.5 million designated as SDM. (Id.)

accordance with the EAR, and seek specific classification-by-classification authorization from BIS. (Id.) Defense counsel estimates it would take thousands of hours to complete this review, including possible consultation with technical experts, and, if there was an error in counsel's classification, counsel would be subject to significant administrative penalties including up to $364,992 per violation, and possible criminal penalties as well. (Id. (citing 50 U.S.C. §§ 4819(b)-(c); 15 C.F.R. §§ 764.2-3, 736.2(b)(10))). Defendants claim that although they have sought assistance from DOJ in securing a license or assisting in the review of the documents to identify the technology at issue, the proposals from DOJ to streamline the process do not protect counsel or Huawei from penalties in the event of an inadvertent disclosure. (Id. at 6).

Defendants argue that BIS's SDM restriction on the 536,000 documents is arbitrary because, in making its DM determination, the DOJ had already concluded that the documents do not implicate any national security concerns, and further, the Department of Commerce "has never even reviewed any of the materials at issue." (ECF No. 451 at 3). Defendants ask the Court to find that, given BIS's restriction on these materials, the prosecution has failed to comply with its obligation to provide discovery to the defense under Rule 16, and has failed to comply with the Protective Order because BIS "subjects the discovery to restrictions extraneous to the Protective Order" and imposes SDM restrictions without "good cause." (Id. at 1-2 (citing P.O. ¶¶ 1, 19-20)).

Citing cases in the Second Circuit, defendants argue that restrictions on criminal defendants' access to discovery is only acceptable under Rule 16 when the restrictions "are supported by a specific and demonstrable need and do not unduly impinge on the defendants' constitutional rights." (Id. at 2 (citing cases)). Defendants contend that here, the restrictions are unacceptable because they impede Huawei's ability to meaningfully participate in and prepare its

defense in this case. (ECF No. 433 at 7). At oral argument, defendants explained that their clients in China must travel to Hong Kong in order to review any of these 536,000 documents that could assist their case. (Tr. at 39:25-40:6). In order to defend itself, defendants insist that Huawei must be able to access all of the government's evidence. (ECF No. 433 at 8).

Thus, defendants argue that because it is the government's burden to rectify the impermissible restriction, the government must apply to BIS to obtain the requisite authorizations. (Id. at 8). Defendants contend that this would not impose as much of a burden on DOJ since it has already reviewed the documents and, in consultation with BIS, should be able to provide whatever technological classification is necessary to obtain a license authorizing disclosures to Huawei. (Id.)

2. The Government's Response

According to the Borman Declaration, since Huawei was listed on the Entity List in 2019, BIS has issued ten (10) authorizations granting Huawei's counsel the authority to release certain technology and software without requesting an application from counsel for a license. (Borman Decl. ¶ 37). In each instance, counsel identified the subject of the authorization request by the applicable Export Control Classification Number ("ECCN"). (Id. ¶¶ 37, 38). According to Mr. Borman, BIS acted expeditiously to grant authorizations, including one authorization sought by letter dated July 3, 2020, which was issued within one business day of the request. (Id. ¶ 39).

In July 2022, Huawei's counsel sought broad authorization from BIS to release all discovery-related materials subject to the EAR "'to [Huawei and Huawei Device USA, Inc.] employees, contractors, witnesses, experts, non U.S.-counsel, or other non-U.S. persons involved in the defense of the proceedings. . . .'" (Id. ¶ 32 (quoting counsel's July 8, 2022 letter (ECF No. 433-1))). Counsel also sought to release all of this technology and software to "persons apparently unrelated to Huawei and largely unidentified," including "'vendors, contractors, and

service providers,'" whether in China or other locations. (Id.) Thus, "regardless of the sensitivity of the technology or software, authorization was requested to "export, reexport, or transfer (in country) any and all technology and software . . . to any country in the world and to any person." (Id. ¶ 32).

With respect to this request for authorization, BIS held multiple virtual meetings with Huawei's counsel, and made multiple requests for the identification of the ECCNs pertinent to the request, but Huawei's counsel refused to provide that information. (Id. ¶ 40). After discussions spanning over a year, Huawei agreed to amend its request to exclude release of the requested material in Belarus, Cuba, Iran, North Korea, Syria, the Russian Federation, and certain regions in Ukraine, but aside from these exclusions, on June 8, 2023, Huawei's counsel insisted on "'the full scope of our July 8, 2022 written authorization request.'" (Id. ¶ 41 (quoting counsel's June 8, 2023 letter)). In connection with this request, Huawei's counsel did not identify the relevant ECCNs, but simply requested authorization consistent with the Protective Order in this case. (Id.)

On October 30, 2023, in its Interim Authorization, BIS authorized certain releases of these materials for purposes of the litigation. The Interim Authorization allowed for the export to listed Huawei entities in China of specific categories of material, namely, (1) technology or software designated as EAR99 or controlled on the CCL in Supp. No. 1 to part 774 of the EAR for Anti-terrorism (AT) reasons only, and (2) technology or software that is the attorney work product of Huawei's attorneys. (Id. ¶ 42). This authorization allows Huawei personnel to receive this technology or software from counsel if related to the litigation without requiring them to leave China. (Id. ¶ 43). In addition, the authorization allowed the release of any

remaining technology or software, so long as it is treated as SDM under the Protective Order.[15] (Id. ¶¶ 42, 44). This limitation was placed on the release of such material because counsel had not identified the specific technology or software for which authorization was being sought. (Id. ¶ 44).

In January 2024, Huawei requested authorization for any technology or software not previously authorized outside the United States by the October 2023 Interim Authorization. (Id. ¶ 46). After BIS informed Huawei that they needed to apply for a license, counsel submitted a license application but did not identify any specific technology or software that was outside the October 2023 Interim Authorization, but instead "identified nearly every ECCN on the Commerce Control List," including items clearly unrelated to the litigation. (Id. ¶ 47). In the absence of specific information, BIS could not make a national security or foreign policy determination. (Id.)

In defense counsel's letter, it is clear that release was sought not only for documents provided by DOJ, but also documents provided by third parties, but the letter did not identify the technology or software sought, nor did it explain why a near worldwide release was warranted. (Id. ¶ 48). BIS returned the license application on March 29, 2024 because it lacked:

> documentation of the technology being requested for export to Huawei; a justification for requesting technology ECCNs that are not related to telecommunications . . .; and information on how the technology listed on this license will be safeguarded and protected from unauthorized disclosure and/or release to unauthorized end users and end uses.

(Id. ¶ 50).

[15] The Interim Authorization language highlights "particular provisions of the Protective Order" – namely, the provisions preventing SDM from being taken outside the United States "except as provided in the Protective Order," and dictating that Huawei may only view SDM in the presence of defense counsel. (ECF No. 433-2 at 1).

In opposing defendants' request, the government argues that it has complied with its obligations under Rule 16 of the Federal Rules of Criminal Procedure, and that BIS, as an independent agency, has a different statutory mandate to not only protect national security, but also foreign policy and economic objectives. The government contends that in the context of Rule 16, the term "government" has been construed to mean the prosecutors in the particular case or the agencies involved in the prosecution, but not the "government" in general. (ECF No. 443 at 4 (citing United States v. Volpe, 42 F. Supp. 2d 204, 221 (E.D.N.Y. 1999))). In United States v. Chalmers, 410 F. Supp. 2d 278, 289 (S.D.N.Y 2006), the court held that other government agencies involved with limited aspects of the prosecution were not considered part of the prosecution team, and the court was "not persuaded that the 'government' for purposes of Rule 16 should be any broader that the 'prosecution team' standard" adopted in the context of Brady. See also United States v. Loera, No. 09 CR 466, 2017 WL 2821546, at *7 (E.D.N.Y. June 29, 2017). The government further argues that in the context of discovery of classified materials, disclosures solely to defense counsel have been found to satisfy the government's discovery obligations, where the defense counsel possesses the necessary clearance, even though the defendant will never have access to the classified discovery. (ECF No. 443 at 5 (citing United States v. Muhanad Mahmoud Al Farekh, No. 15 CR 268, 2016 WL 4444778, at *3 (E.D.N.Y. Aug. 23, 2016)). See also United States v. Zazi, No. 10 CR 60, 2011 WL 2532903 at *5 (E.D.N.Y. June 24, 2011) (holding that the provision of summaries to defense counsel satisfied the government's obligations in a manner that protects national security).

The government contends that not only is BIS not part of the prosecution team, BIS is not acting pursuant to direction from the prosecution team, is not a party to the Protective Order, and has not aided in crafting trial strategy. (Id. (citing United States v. Meregildo, 920 F. Supp. 2d

434, 442 (S.D.N.Y. 2013))). Although the prosecution team has conferred with BIS in an effort to facilitate BIS communications with defense counsel, the prosecution team has no legal authority to direct BIS to exempt defendants from the export control laws and would be unable to comply with a court order requiring the government to cause BIS to issue a broader license to Huawei. (Id.) Indeed, the DOJ is not part of the review process set out in ECRA or the EAR, so even if the government were to make such a request, it could not compel BIS to comply. (Id. at 5-6). Moreover, the government notes that any "'determination by the Court that an export control authorization from BIS is made irrelevant by the Court's Protective Order would undermine BIS's statutory authority to regulate export controls pursuant to U.S. national security and foreign policy concerns as well as the ability of BIS's interagency partners to review and assess any license application.'" (Id. at 6 (quoting Borman Decl. ¶ 52)).

At oral argument, the government challenged defendants' argument that the government's initial designation of the materials as DM made BIS's restriction "'arbitrary,'" emphasizing that BIS "is considering different equities," and its licensing review process is "not the same exercise" as DOJ's evaluation of the materials as they relate to the instant case. (Tr. at 42:15-24). BIS is tasked with not only protecting national security, but also "foreign policy and economic objectives," and therefore the fact that BIS made a determination regarding the sensitive nature of the materials that was distinct from DOJ's evaluation does not itself make BIS's determination arbitrary. (Id. at 42:24-43:1).

Moreover, the government disputes defendants' assertion that the government is the principal party responsible for obtaining the license from BIS and instead, takes the position that because defense counsel seeks to export discovery materials containing technology, including technology belonging to the victims of intellectual property theft, defendants' counsel must first

obtain a license from BIS. (ECF No. 443 at 3). The government further contends that it has satisfied its obligations by producing discovery to defendants' counsel (id. at 6 (citing United States v. Cobb, 544 F. Supp. 3d 310, 330 (W.D.N.Y. 2021))), and, based on the October 30, 2023 Interim Authorization issued to Huawei, personnel and witnesses may access DM containing technology without obtaining additional licenses, so long as they treat these materials in accordance with the treatment of SDM under the Protective Order. (Id.) Since the Protective Order is silent on the issue of obtaining licenses, the government argues that the government's designation of certain material as DM has no bearing on Huawei's obligation to comply with laws enforced by the Department of Commerce, an agency distinct from DOJ and the prosecution team. (Id. at 7).

C. Analysis

Under Rule 16 of the Federal Rules of Criminal Procedure, the prosecution has an obligation to produce certain discovery materials to the defense, including certain relevant documents. United States v. Smith, 985 F. Supp. 2d at 521-22 (collecting cases); see generally Fed. R. Civ. P. 16(a). Courts have suggested that this obligation necessitates the production to defendants themselves, as well as defense counsel. See United States v. Baker, 20 CR 288, 2020 WL 4589808, at *4 (S.D.N.Y. Aug. 10, 2020) (noting that, "[i]n criminal cases, the accused has a personal interest in making his or her best defense" (citing Faretta v. California, 522 U.S. 806, 819 (1975))). Any restriction on discovery must be supported by "good cause." Fed. R. Crim. P. 16(d)(1). Courts have held that cases implicating national security or witness safety demonstrate "good cause" sufficient to restrict defendants' access to certain discovery materials. See, e.g., United States v. Castricone, 2021 WL 841405, at *2 (citing concerns for victim's safety in allowing a restriction on certain documents for the defendant to only view in the presence of

defense counsel); United States v. Muhanad Mahmoud Al Farekh, 2016 WL 4444778, at *3 (allowing production of classified summaries to defense counsel given risks to national security).

In this case, the prosecution has produced all of the materials at issue to defense counsel (ECF No. 443 at 6); this is not a question of whether the government is withholding particular documents from defendants or even preventing defendants themselves from accessing this discovery. The issue is whether certain documents should be considered SDM and access to these documents should be subject to the restrictions imposed under that category. Defendants contend that the prosecution must show "good cause" to maintain the SDM designation of these documents. (ECF No. 433 at 7). However, the SDM designation was not imposed by the prosecution; these materials were designated as SDM by BIS in an effort to allow defendants' review of documents in the absence of the statutorily required license under ECRA and the EAR. 50 U.S.C. § 4814(c); 50 U.S.C. § 4822(c); see also 15 C.F.R. § 750. While the prosecution may have determined that the 536,000 documents at issue were discoverable as DM, a license was still required to export documents containing EAR-restricted technology to Huawei, a listed entity, and therefore, these documents were still subject to further review by BIS. (See ECF No. 433 at 4; ECF No. 443 at 3). As the prosecution explained, the factors considered by BIS and other government agencies in evaluating these materials are distinct from the prosecution's confidentiality evaluation under Protective Order. (Tr. at 42:15-43:1). Thus, the fact that DOJ has determined these materials to be DM under the Protective Order does not override the independent review responsibilities of BIS. The prosecution complied with Rule 16 by producing to the defense these materials in a manner consistent with its obligations to defendants, and need not demonstrate good cause for the BIS designation that was outside the prosecution's control.

To the extent the defendants seek an order requiring the prosecution to obtain the appropriate license, the prosecution confirmed that neither they, nor the Department of Justice itself, have any authority over BIS and its licensing decisions; thus, a court order requiring the government to apply for a license that complied with the instant case's Protective Order would not alter BIS's review process. (ECF No. 443 at 5; Tr. at 46:20-25).

Moreover, it is unclear that, had the defendants provided the information required by BIS – including identification of the specific technology or software being requested for export to Huawei, rather than requesting "nearly every ECCN" on the CCL (Borman Decl. ¶ 47), and the reason for requesting a license for technology not related to telecommunications – BIS would not have issued a license or made some other accommodation to defendants' request, such as the earlier authorizations. Indeed, it should be emphasized that in 2023, rather than require defendants to actually obtain a license, BIS agreed to what the government terms an "extraordinary measure" to allow defendants to circumvent BIS's usual licensing process as to the 536,000 DM documents, so long as defendants treated the material as SDM. (Tr. at 42:5-6). The defendants cite the burden of reviewing the documentation and the concern of possible penalties in the event of misclassification,[16] but those concerns do not demonstrate that BIS's determination that this information should be treated as SDM is "arbitrary." If there are specific documents that defendants believe should be otherwise classified as DM, BIS has indicated a

[16] As to defendants' concerns over exposure to criminal and civil penalties in seeking further authorizations or licensure from BIS, the Court notes that these penalties are an inherent part of the applicant's burden under the statute. While it is unclear whether these penalties would apply equally to the authorizations issued by BIS in this case, the defendants seemingly have already faced exposure to these penalties in their use of documents pursuant to their current authorizations. In addition, even under the normal statutory regime, the imposition of penalties is not automatic, and there are mitigating factors that would be considered as set forth in the statute. See 50 U.S.C. § 4819(c)(3) (explaining that, in imposing civil penalties, the Secretary of Commerce may consider "factors such as the seriousness of the violation, the culpability of the violator, and such mitigating factors as the violator's record of cooperation with the Government in disclosing the violation"); 50 U.S.C. § 4819(b) (indicating that the standard for imposing criminal penalties is willfulness).

willingness to consider extending authorization once they have had the opportunity to review the specific technology and related concerns.[17]

In addition, the Court finds persuasive the case authority that construes the "government" for purposes of Rule 16 to be limited to the prosecution and does not include BIS, a part of the Department of Commerce, a separate administrative agency from the Department of Justice. (ECF No. 443 at 5 (citing United States v. Meregildo, 920 F. Supp. 2d at 442)). The Protective Order entered in this case does not bind BIS to its terms and does not override BIS's statutory mandate to carry out its responsibilities under ECRA and the EAR. Indeed, under Section 758.3 of the EAR, "[a]ll parties that participate in transactions subject to the EAR must comply with the EAR." 15 C.F.R. § 758.3. As a party participating in the export of potential "technology" subject to the EAR, the defense must comply with the EAR irrespective of any conflicts with the Protective Order's terms or discovery obligations. (ECF No. 443 at 3). For this Court to conclude otherwise would "undermine BIS's statutory authority to regulate export controls pursuant to U.S. national security and foreign policy concerns." (Borman Decl. ¶ 52).

In finding that the government has satisfied its obligations under Rule 16, the Court notes that the SDM designation still allows for defendants' access to the discovery materials, under the restrictions set forth in the Protective Order. (ECF No. 433 at 5). Defendants have not articulated any concrete harm imposed by this designation and the refusal of BIS to bypass its evaluation procedures beyond the inconvenience of forcing their clients to travel from China to review the material; indeed, at oral argument, defendants conceded their argument was largely a "technical" one. (Tr. at 39:11-16). Courts in this circuit have found that the government

[17] The Court notes that, like the defendants' initial request to release all of this technology in countries around the world, including Cuba, Iran, North Korea, Syria, and the Russian Federation, the request for a license or authorization to declassify wholesale all of the documents produced without regard to concerns of national security or economic considerations, or even relevance, appears unwarranted without further explanation.

complied with Rule 16 in cases where defendants were permitted to view certain discovery only in the presence of defense counsel, see United States v. Castricone, 2021 WL 841405, at *2, and in certain cases, have even concluded that defendants would not be allowed to access the material at all when it implicated national security concerns. United States v. Muhanad Mahmoud Al Farekh, 2016 WL 4444778, at *3.

Here, Huawei was placed on the EAR Entity List due to "'reasonable cause to believe that Huawei has been involved in activities contrary to the national security or foreign policy interests of the United States.'" (Borman Decl. ¶ 30 (citing 84 Fed. Reg. 22961)). In addition, although defendants complain that BIS imposed a blanket SDM restriction on documents it had not yet reviewed and that may not actually warrant such restriction, the Court notes that this was an apparent concession by BIS to allow defendants sufficient access to the material without the delay of the usual review process, while still addressing BIS's security concerns. (See id. ¶ 40 (noting that, in determining appropriate authorizations, BIS was working to satisfy defendants' "litigation needs" without "undermining U.S. national security . . . concerns")). Thus, even if BIS or the government did have an obligation to show good cause for the current SDM restrictions on these documents, they likely would be able to make a successful showing.

In light of the above, defendants' request for the Court to provide relief from BIS's licensing requirements is denied.

CONCLUSION

For the reasons stated above, defendants' SDM Motion is granted in part and denied in part, and defendants' BIS Motion is denied.

Defendants' request for the SDM designation to allow for remote access in Mainland China under defendants' proposed protocol is denied, and defendants are Ordered to comply with the Protective Order's SDM terms as they currently stand.

Defendants' request for a de-designation review period is granted in part and denied in part. Upon defendants' challenge to a confidentiality restriction, the government shall respond within 60 days or else request an extension of time by agreement with defendants or from the Court. The Court denies the defendants' request for a 21-day response period.

Defendants' BIS Motion is denied. To the extent defendants wish to apply for additional licensing or authorizations from BIS, the burden to do so shall remain with defendants.

SO ORDERED.

Dated: Brooklyn, New York
November 4, 2024

/s/ Cheryl L. Pollak
Cheryl L. Pollak
United States Magistrate Judge
Eastern District of New York